高技术通讯 2010 年 第 20 卷 第 6 期:585 ~ 589

doi:10.3772/j.issn.1002-0470.2010.06.006

基于量子纠错理论的数字水印技术①

孙建国②* 门朝光* 姚爱红* 张国印* 林 锰**

(*哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

(**哈尔滨工程大学理学院 哈尔滨 150001)

摘 要 针对数字水印算法通用性及应用性较差的问题,提出了一种基于量子纠错理论的数字水印技术,描述了量子数字水印算法的实现流程,并以文本介质为例进行了实验。该技术利用量子的相干性和力学叠加原理,将量子错误编码作为水印嵌入介质中,并通过编码纠错的途径来提取水印。本文感官测试表明,该数字水印技术的抗攻击能力突出,是基于文本格式水印的 4 倍;在攻击测试中,量子水印同其它水印技术相比,误码率平均降低了 18.06%。实验表明此算法具有很好的通用性及鲁棒性能。

关键词 信息隐藏,数字水印,量子理论,纠错编码,通用性

0 引 言

随着数字技术和互联网的迅速发展,图像、音频、视频等形式的多媒体数字作品在网络上广泛传播,数字水印(digital watermarking)技术作为信息隐藏(information hiding)技术领域的重要分支,正成为信息领域的一个研究热点[1,2]。Ozdemir 等人在 2005 年发表的关于水印嵌入的论文[3]首次提出用量子编码携带隐藏信息的新技术,开辟了量子信息隐藏的研究方向,但只给予了简短的可行性说明,并未进行深入讨论。众所周知,物理量子具有相干性、纠缠性等特性,利用这些特性能够较好地解决隐藏算法鲁棒性和隐藏性二者之间的矛盾,如果同步地重复嵌入数据则可扩充水印容量,进而获得鲁棒性、不可感知性及容量三者间的最佳平衡点[4]。

本文提出一种通用的基于量子理论的数字水印技术,该技术将水印载体空间映射为一个有 N 个量子位的 Hilbert 空间[5],水印嵌入操作是 Hilbert 空间内一次 k 个量子位发生的随机错误(独立消相干),水印提取通过对量子位纠错操作实现。由于量子态具有前述特性,量子数字水印在性能方面有较大改善。

1 量子编码方案

1.1 基本概念

定义 1 量子:微观系统中能量的一个力学单位,现代物理将微观世界中的所有的微观粒子(如光子、电子、原子等)统称为量子。

定义 2 量子的相干性:在微观世界中,量子有许多特有的状态属性,即量子态的叠加性,量子态的纠缠,量子态的不可克隆,以及测量导致量子态"塌缩"等现象。这些现象来自量子间存在的相互干涉,即所谓的量子相干性。

定义 3 量子纠缠:n 个量子在特定的环境下可以处于较稳定的纠缠状态,对其中某个子系统的局域操作会影响到其余子系统的状态,其中 $n > 1$,$n \in \mathbf{N}^*$。

定义 4 消相干[6]:由于受到环境的影响,量子系统会出现量子位能量耗散的现象。量子干涉性消失,量子信息散失在无法控制的环境中的现象称为量子消相干。

下式分别表示经典编码与量子编码

$$\alpha \mid 0 > \rightarrow \alpha \mid 0 > + \upsilon \mid 1 >$$

$$\beta \mid 1 > \rightarrow \beta \mid 1 > + \delta \mid 0 > \quad (1)$$

$$\mid \alpha + \delta \mid^2 + \mid \beta + \upsilon \mid^2 = 1 \quad \upsilon, \delta \in C \quad (2)$$

其中 α, β 表示经典编码的变量;υ, δ 表示量子变量。

与经典编码不同(如式(1)),量子编码的错误可能不会造成状态的完全转换[7](0,1 的变换),有可能只会使量子位发生一定的偏移(如式(2))。

① 中央高校基本科研业务费专项(HEUCF100606)资助项目。

② 男,1981 年生,博士生,讲师;研究方向:信息安全,数字水印;联系人,E-mail: sunjianguo@hrbeu.edu.cn.

(收稿日期:2009-03-17)

1.2 量子编码方案

设一个物理量子态 $|\psi>$ 可能变换的情形包括：

(1)量子位反转错，记为 X；

(2)量子位相翻转，记为 Z；

(3)位反转错与位相翻转同时发生，记为 Y。

此外，约定一般情况下未发生错误的量子状态为 I。若设量子态 $|\psi>$ 包含 k 个量子位，则 $|\psi>$ 可表示为

$$|\psi> = \alpha_0|0\Lambda 00> + \alpha_1|0\Lambda 01> + \alpha_2|0\Lambda 10> + \Lambda + \alpha_{2^k-1}|1\Lambda 11> \tag{3}$$

此时，若 m 量子位出错（$m \leqslant k$），出错类型集合记为 $\{X, Y, Z\}$，则 $[[n, k]]$ 表示使用 n 位的纠错编码来处理 k 位量子串中的 m 位错误。通过图 1 的映射规则，可以看到隐藏算法转变为量子纠错的过程。

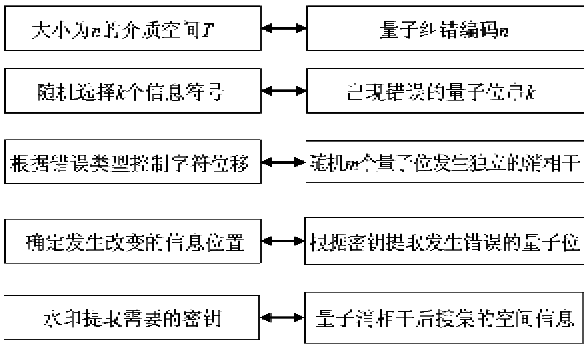

图 1 数字水印技术与量子纠错编码的映射关系图

2 量子数字水印方案

2.1 水印嵌入方案

首先，k 量子位按序同随机选择的 $n-k$ 个未出错量子融合，形成大小为 n 的空间；定义引入的 $n-k$ 个量子态为经典状态 $|0>$ 态，则有如下等式成立：

$$|\psi>_H = f(\sum_{i=1}^{n-k}|0>_i, |\psi>) \tag{4}$$

其中 $|\psi>_H$ 为 $|\psi>$（k 量子位的原始量子态表示）在新空间中的量子态表示。对每一个量子态捆绑一个操作单元 C。则空间中的量子错误可表示为

$$E_H = \sum_{i=1}^{n} C_i \times X, Y, Z, N = E_1E_2E_3\Lambda E_{n-1}E_n \equiv XNY\Lambda ZN \tag{5}$$

根据量子态变换操作 $\{X, Y, Z, I\}$ 的定义，随机将 m 个量子比特进行独立的消相干，并将位置信息（E_H）存储到密钥 Key。在 Hilbert 空间内，量子出错可以表示为量子对应算子的线性组合。根据量子相干性原理，此时系统的出错表现为“纠缠态”[7]，即 $|\psi>_H E_H|E'>$；文字表述为系统 $|\psi>_H$ 在环境 E' 的作用下，产生错误的量子比特串 E_H。

2.2 水印检测及提取方案

为纠正量子错误，首先应确定出错位置，因此，需引入定位算子 T_e 和辅助算子[8]。定位算子用于指明出错位，辅助算子是为了克服量子的不可测量特性引入的，通常定义为经典状态 $|0>$ 或 $|1>$。在实际的纠错环境中，量子系统存在等式

$$T_e(|\psi>_H, (E_H, |0>)) = |x> \cdot (E_x|E_H) \tag{6}$$

其中 x 为二进制字符串。

$|x>$ 既表达了新的量子态，也指明了量子出错的位置信息 E_x。在环境 E' 的作用下，指错运算的输出结果是[8]：

$$T_e(|\psi>_H\bar{E}_H|E'>, (E_H, |0>)) = |E'>|\psi>_H|x> \cdot E_x|E_H \tag{7}$$

对量子态的测量将发生态坍缩，因此，测量 $|x>$ 态能够使整个表达式所代表的量子态被确定下来；输出为 $|E'>|\psi>_H|x_0> \cdot E_{x_0}$。此时 x_0 为已知（非 $|0>$ 即 $|1>$）。量子错误编码定义为“$E_{x_0} = E_1E_2E_3AE_{x_0-1}E_{x_0}$”，则 E_{x_0} 的可逆运算为

$$(|E'\rangle|\psi\rangle_H|x_0\rangle \cdot E_{x_0}) \cdot E_{x_0}^{-1} = |E'>|\psi>_H|x_0> \tag{8}$$

环境 $|E'>$ 是状态无关的，$|x_0>$ 为经典状态，这样，重新获得了 $|\psi>_H$，而错误编码 E_H 正是需要提取的水印信息。值得强调的一点是：只要量子比特独立地发生消相干，那么对任意出错量子位的纠错方案都会有效。

3 量子数字水印算法及分析

量子数字水印算法分为嵌入和提取两个部分。

对于嵌入过程来说，算法的输入为介质空间 T，$|T| = n$；数字水印编码 L，$|L| = k$（$n \geqslant k$），其中 L_i（$1 \leqslant i \leqslant m$）表示一个量子位。

算法的输出为嵌入水印后的介质 T_L。其中，水印串 L 对应的量子态 $|\psi>_L$ 为

$$|\psi>_L = |\psi>_1 \otimes |\psi>_2 \otimes \cdots \otimes |\psi>_m \tag{9}$$

根据上节所述的量子纠错原理，可知在 Hilbert

空间的构造过程中,引进的冗余量子为经典状态 $|0>$。按照 $|\psi>_L$ 的内容构造出错编码 E_T,调整空间 T 内的 $m(m=||\psi>_L|)$ 个量子态发生 υ 或 δ 大小的量子偏移($\delta,\upsilon \leqslant |\psi>_L$),形成一个大小为 $[[n,k]]$ 的纠缠编码。E_H 作为密钥记录了量子出错位。这里做了一次规约:

$$|E_T|=m$$
$$|\psi>_T=|\psi>_1|\psi>_1\Lambda|\psi>_k$$
$$|E'>=|E'>_{k+1}|E'>_{k+2}\Lambda|E'>_{n-k} \quad (10)$$

按照 E_H 提供的出错信息进行了重复嵌入,以此提高水印的鲁棒性,同时,重复嵌入也扩充了水印容量。

如前所述,对于水印串 $L(|L|=k)$,发生错误的量子位数为 $m(m<k)$。若将水印串随机嵌入空间 T 内 3 次,则水印损毁的概率是 $\left(\frac{1}{m}\right)^3$。只有量子态 L_i 的 3 个嵌入位 $L_i|E_T$ 被全部破坏,L_i 才无法提取。水印若嵌入 n,则水印失效的概率仅为 $\frac{1}{m^n}$。

4 实验及分析

文本数字水印的最大研究难点在于无法解决水印容量、鲁棒性和隐藏效果三者之间的矛盾。我国文本数字水印技术起步较晚,直至 2000 年才出现一些研究型的论文。选择文本作为算法实验对象。

4.1 水印嵌入效果展现

所选择的文本空间共 81 个字符(不计标点符号)。定义一个长度为 8 的水印字符串,随机产生 m($m \leqslant 8$)个错误,根据量子错误(υ 或 δ)调整字符的水平和纵向偏移量,并将水印重复嵌入 3 次。由前节的定义可知,水印容量为 48b,密钥容量为 404b,水印提取失败的概率仅为 0.042969。图 2 给出了水印嵌入实例。

从水印的提取算法可以很直观看出,水印的提取过程主要利用了量子的不可测量和不可克隆的相干性原理,通过局部测量和检测器的原理来进行水印串的量子到经典二进制数串的转化.

(a)原始文本

从水印的提取算法可以很明显看出,水印的提取过程主要利用了量子的不可测量和不可克隆的相干性原理,通过局部测量和检测器的原理来进行水印串的量子到经典二进制数串的转化.

(b)嵌入水印的文本

图 2 水印嵌入实例

*在嵌入过程中,扩大了量子的偏移量,使水印信息能够明显体现出来

4.2 水印攻击测试

水印攻击测试主要包括视觉检测和攻击测试。

参照视觉检测的通常手段,分别使用基于行间距编码水印和量子水印对朱自清的"荷塘月色"进行处理,其中量子水印被嵌入 4 次。实验中,随机抽取 100 名学生进行视觉测试,将其分成 4 组:A,B 组提供包含量子水印的文章。A 组被告知该篇文章包含水印,是通过字符调整实现的,并为其提供原始文本,要求在尽可能短的时间内找出水印或者规律;B 组不告知包含水印信息,仅提示找出文本异常;C,D 两组提供包含行间距编码数字水印的文章。C 组仅告知存在文本异常,D 组则提示包含水印,且通过调整行间距嵌入,并为其提供原始文本。测试时间限定 3 分钟,每 30 秒统计一次数据。

实验结果如图 3 所示。量子水印的抗攻击能力是格式水印的 4 倍以上。重复性和随机性加大了水印的容量,所以抗攻击能力也获得了大幅提高。

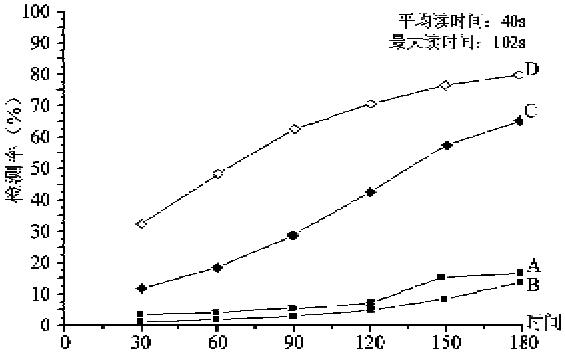

图 3 视觉检测结果

常见的针对数字水印的攻击方法有 21 种[9]。本文选取 8 种。在网络上搜索了 WORD,PDF,TXT 文件 208 篇,文件总容量 101.56M,平均容量 499.98k 文件容量从 10k 到 2M 不等。随机组织了长度为 1000 的量子水印串,发生 m 位错误。保证一个页面的(大小为 21cm × 29.7cm)水印容量至少为 m。水印的攻击操作均基于 Matlab7.0 仿真实现。

分别选择基于语义替换[10]、字符间距[11]、行间距[11]、云模型[12]的数字水印参与对比。结果如表 1 所示。在保证嵌入率(水印同编码空间的比值)均等的情况下,通过误码率(水印提取的错误编码位数同水印编码总长度的比值)指标对各算法进行评价。

表1 攻击效果测试

攻击类型		不同类型数字水印的误码率(%)					
攻击内容	说明	量子水印	语义替换[10]	字符间距[11]	行间距[11]	云模型[12]	优化幅度
翻转	–	0	0	2.14	0	0	2.14
旋转	60° 顺时针	0	0	2.14	0	0	2.14
	90° 顺时针	0	0	2.41	0	0	2.41
	180°逆时针	0	0	2.11	0	0	2.11
旋转和尺寸缩放	60°,30%	0	0	9.82	1.76	2.97	9.82
	90°,50%	0	0	13.66	6.98	7.12	13.66
	180°,70%	0	0	10.23	23.84	26.7	26.7
线性变换	15%	1.54	2.86	2.16	8.92	10	8.46
	45%	3.6	5.12	3.15	18.71	17.86	15.11
缩放	30%	0	0	9.82	2.46	1.04	9.82
	50%	0	0	13.66	7.33	9.77	13.66
	80%	0	0	10.23	32.4	24.9	32.4
行移除	10	3.12	11.19	4.16	15.9	22.31	19.19
	20%	5.68	13.2	7.82	22.76	25.66	19.98
	30%	8.16	34.28	15.36	40.55	32.07	31.39
非线性答移除	10%	7.58	12	11.2	26.7	23.28	18.12
	20%	9.33	14.26	15.9	32.18	29.03	22.85
	30%	11.07	33.97	23.68	56	40.38	44.93
拼贴	5%	4.08	12.45	5.19	34.28	42.09	38.01
	10	8.89	44.6	10.65	41.58	55.8	46.91

定义5 误码率:水印的实现过程中,接收的信息发生错误的概率若为 $p(0 < p < \frac{1}{2})$,则正确接收的概率为 $1-p$,即信息接收前后不相同的概率是 p,p 称为误码率。

实验结果表明:相对于其它4类文本数字水印,量子水印的平均误码率降低了18.06%。对于格式攻击,量子水印都变现出了很好的鲁棒性。而内容攻击对水印有一定破坏作用,但水印多次嵌入降低了这种损失。算法在应对拼贴,移除等攻击时,都表现了很好的可恢复性。

5 结 论

本文基于量子相干性生产数字水印,利用量子纠错完成水印提取。基于文本型介质的水印实验表明量子数字水印检测的错误率得到了大幅降低。作为一种通用的水印算法,量子数字水印方案具有很强的可映射性,在图像,视频等具体应用领域均有研究意义和应用前景。本研究的下一步工作是尝试建立一个基于量子理论的水印评价模型。

参考文献

[1] Xu D H, Zhu C Q, Wang Q S. A survey of the research on digital watermark for the vector digital map. *Geomatics World*, 2007, 12(6):42-48

[2] 马桃林,顾种,张良培.基于二维矢量数字地图的水印算法研究.武汉大学学报(信息科学版),2006,31(9):792-294

[3] Ozdemir T, Yamamoto M, Koashi N. Embedding watermark in qubit strings using error correction coding. In: Proceedings of the 2005 European Quantum Electronics Conference, Munich, Germany, 2005, 1208-1210

[4] Pan Z H, Li Z J, Gong Z X. A survey of digital watermarking. *Computer & Digital Engineering*, 2008, 36(4): 119-121,133

[5] Zak M. Quantum algorithms in Hilbert database. *International Journal of Theoretical Physics*, 2003, 42(9):2061-2069

[6] Tang Z X, Zhang D Y. Quantum coherence and decoherence. *Journal of Laser*, 2003, 24(6):39-42

[7] Tannor D J, Sklarz S E. Quantum computation via local control theory: direct sum vs. direct product Hilbert spaces. *Chemical Physics*, 2006, 332(2): 87-97

[8] 蔡乐才. 量子纠错码的研究. 四川理工大学学报(自然科学版, 2004, 17(3):90-94

[9] 尹浩,林闯,邱锋等.数字水印技术综述. 计算机研究

与发展, 2005,42(7):1093-1099
[10] Voiqt M, Yang B, Busch C. Reversible watermarking of 2D - vector data. In: Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security, Magdeburg, Germany, 2004. 160-165
[11] 王涛. 坐标几何中的水印隐藏算法设计与实现:[硕士学位论文]. 北京:北京邮电大学,2003. 40-43
[12] 赵东宁, 张勇, 李德毅. 基于云模型的文本数字水印技术. 计算机应用,2003, 增刊 2. 100-102

Digital watermarking based on quantum error correction coding

Sun Jianguo*, Men Chaoguang*, Yao Aihong*, Zhang Guoyin*, Lin Meng**
(* College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)
(** College of Science, Harbin Engineering University, Harbin 150001)

Abstract

To solve the problem that most digital watermarking algorithms have the poor performance on the application and universality, a novel watermarking technology based on the theory of quantum error correction is proposed. According to the principles of quantum coherence and mechanical superposition, the watermark is embedded into the carrier in the format of quantum error codes, and it is extracted by the approach of quantum error correcting. It is introduced that the embedding and extraction of the quantum digital watermarking algorithm in this paper. Further, the text is examined as a carrier instance for this algorithm. The sensory test results indicate that the anti-attack capability of the algorithm is 4 times of the text-formatted watermarking. On attack tests, the error-coding rate of the quantum watermarking decreased an average of 18.06 percent compared with others. The experiment shows that this algorithm has a better performance on universality and robustness.

Key words: information hiding, digital watermarking, quantum theory, error coding correction, universal